PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 3/00 | A2

(11) International Publication Number: **WO 98/51032**

(43) International Publication Date: 12 November 1998 (12.11.98)

(21) International Application Number: PCT/CA98/00418

(22) International Filing Date: 4 May 1998 (04.05.98)

(30) Priority Data:
9709135.9 2 May 1997 (02.05.97) GB

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard, West, Mississauga, Ontario L5R 3L7 (CA).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: VANSTONE, Scott, A. [CA/CA]; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA). JOHNSON, Donald [US/US]; 7684 Knightshayes Drive, Manassas, VA 20111 (US). LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA). VADEKAR, Ashok, V. [CA/CA]; 2006–700 Constellation Drive, Mississauga, Ontario L5R 3G8 (CA).

(74) Agents: PILLAY, Kevin et al.; Orange & Associates, Toronto Dominion Bank Tower, Suite 3600, Toronto–Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: TWO WAY AUTHENTICATION PROTOCOL

(57) Abstract

A method of authenticating a pair of correspondents C, S to permit the exchange of information therebetween, each of the correspondents having a respective private key, e, d and a public key, Q_u and Q_s derived from a generator element of a group and a respective ones of the private keys, e, d, the method comprising the steps of: a first of the correspondents C generating a session value x; the first correspondent generating a private value t, a public value derived from the private value t and the generator and a shared secret value derived from the private value t and the public key Q_s of the second correspondent; the second correspondent generating a challenge value y and transmitting the challenge value y to the first correspondent; the first correspondent in response thereto computing a value h by applying a function H to the challenge value y, the session value x, the public value an of the first correspondent; the first correspondent signing the value h utilizing the private key e; the first correspondent transmitting to the second correspondent the signature including the session value x, and the private value t; and the second correspondent verifying the signature utilizing the public key Q_u of the first correspondent and whereby verification of the signature authenticates the first correspondent to the second correspondent.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/CA 98/00418

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G07F H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 272 755 A (MIYAJI ATSUKO ET AL) 21 December 1993 see the whole document ---	1-17
A	EP 0 461 983 A (FRANCE TELECOM ;TELEDIFFUSION FSE (FR); PHILIPS NV (NL)) 18 December 1991 see the whole document ---	1,16,17
A	SCHNORR C P: "EFFICIENT SIGNATURE GENERATION BY SMART CARDS" JOURNAL OF CRYPTOLOGY, vol. 4, no. 3, 1 January 1991, pages 161-174, XP000574352 see the whole document --- -/--	1,16,17

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
21 October 1998	29/10/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Guivol, O

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Intern ial Application No
PCT/CA 98/00418

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	BELLARE M ET AL: "KEYING HASH FUNCTIONS FOR MESSAGE AUTHENTICATION" ADVANCES IN CRYPTOLOGY - CRYPTO '96, 16TH. ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE SANTA BARBARA, AUG. 18 - 22, 1996. PROCEEDINGS, no. CONF. 16, 18 August 1996, pages 1-15, XP000626584 KOBLITZ N (ED) see the whole document ---	1,16,17
A	EP 0 440 800 A (NTT DATA TSUSHIN KK) 14 August 1991 see abstract; claims ---	1
A	WO 89 11706 A (NCR CO) 30 November 1989 see the whole document ---	1
A	EP 0 225 010 A (BRITISH TELECOMM) 10 June 1987 see abstract; claims; figures ---	1
A	KENJI KOYAMA ET AL: "ELLIPTIC CURVE CRYPTOSYSTEMS AND THEIR APPLICATIONS" IEICE TRANSACTIONS ON INFORMATION AND SYSTEMS, vol. E75 - D, no. 1, 1 January 1992, pages 50-57, XP000301174 see the whole document ---	
A	WO 93 20538 A (TELSTRA CORP LTD ;ZUK EDWARD ANDREW (AU)) 14 October 1993 -----	

3

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Intern al Application No
PCT/CA 98/00418

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5272755 A	21-12-1993	JP 5181418 A	23-07-1993
		US 5351297 A	27-09-1994
EP 0461983 A	18-12-1991	FR 2663141 A	13-12-1991
		DE 69108786 D	18-05-1995
		DE 69108786 T	16-11-1995
		JP 6084026 A	25-03-1994
		US 5218637 A	08-06-1993
EP 0440800 A	14-08-1991	JP 2731945 B	25-03-1998
		JP 3007399 A	14-01-1991
		WO 9014962 A	13-12-1990
WO 8911706 A	30-11-1989	AU 622915 B	30-04-1992
		AU 3733589 A	12-12-1989
		CA 1321649 A	24-08-1993
		EP 0374225 A	27-06-1990
		JP 2504435 T	13-12-1990
		US 4935962 A	19-06-1990
EP 0225010 A	10-06-1987	NONE	
WO 9320538 A	14-10-1993	AU 671986 B	19-09-1996
		AU 3818093 A	08-11-1993
		CA 2133200 A	14-10-1993
		EP 0634038 A	18-01-1995
		JP 7505270 T	08-06-1995
		SG 46692 A	20-02-1998
		US 5745571 A	28-04-1998

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G07F 7/10

A3

(11) International Publication Number: WO 98/51032

(43) International Publication Date: 12 November 1998 (12.11.98)

(21) International Application Number: PCT/CA98/00418

(22) International Filing Date: 4 May 1998 (04.05.98)

(30) Priority Data:
9709135.9 2 May 1997 (02.05.97) GB

(71) Applicant *(for all designated States except US)*: CERTICOM CORP. [CA/CA]; Suite 103, 200 Matheson Boulevard, West, Mississauga, Ontario L5R 3L7 (CA).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: VANSTONE, Scott, A. [CA/CA]; 539 Sandbrook Court, Waterloo, Ontario N2T 2H4 (CA). JOHNSON, Donald [US/US]; 7684 Knightshayes Drive, Manassas, VA 20111 (US). LAMBERT, Robert, J. [CA/CA]; 63 Holm Street, Cambridge, Ontario N3C 3N3 (CA). VADEKAR, Ashok, V. [CA/CA]; 2006–700 Constellation Drive, Mississauga, Ontario L5R 3G8 (CA).

(74) Agents: PILLAY, Kevin et al.; Orange & Associates, Toronto Dominion Bank Tower, Suite 3600, Toronto–Dominion Centre, P.O. Box 190, Toronto, Ontario M5K 1H6 (CA).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

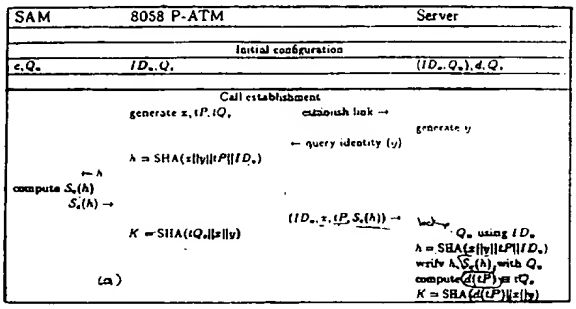
Published
With international search report.

(88) Date of publication of the international search report:
4 February 1999 (04.02.99)

(54) Title: TWO WAY AUTHENTICATION PROTOCOL

(57) Abstract

A method of authenticating a pair of correspondents C, S to permit the exchange of information therebetween, each of the correspondents having a respective private key, *e*, *d* and a public key, Q_u and Q_s derived from a generator element of a group and a respective ones of the private keys, *e*, *d*, the method comprising the steps of: a first of the correspondents *C* generating a session value *x*; the first correspondent generating a private value *t*, a public value derived from the private value *t* and the generator and a shared secret value derived from the private value *t* and the public key Q_s of the second correspondent; the second correspondent generating a challenge value *y* and transmitting the challenge value *y* to the first correspondent; the first correspondent in response thereto computing a value *h* by applying a function *H* to the challenge value *y*, the session value *x*, the public value an of the first correspondent; the first correspondent signing the value *h* utilizing the private key *e*; the first correspondent transmitting to the second correspondent the signature including the session value *x*, and the private value *t*; and the second correspondent verifying the signature utilizing the public key Q_u of the first correspondent and whereby verification of the signature authenticates the first correspondent to the second correspondent.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

P-ATM	Service Server	KDS
Initial configuration		
ID_u $SAK = TDES^{E}_{K_V}(ID_u)$	d_s, Q_s	ID_u, Q_s, K_V
Registration/Binding		
Register		Bind ID_u to Q_s $SAK = TDES^{E}_{K_V}(ID_u)$ $ESK = DES^{E}_{SAK}(ID_u, Q_s)$
	Update database with ID_u, ESK	$\leftarrow M$ $M = (ID_u, ESK)$
First connection		
	connect $\rightarrow$	
	$\leftarrow$ query ID (y)	generate y
	$(ID_u, x, tP) \rightarrow$	lookup ID_u
	$\leftarrow ESK$	
Decrypt $(ID, Q_s) = DES^{D}_{SAK}(ESK)$ Verify $ID \equiv ID_u$ Program Q_s		

Figure 7

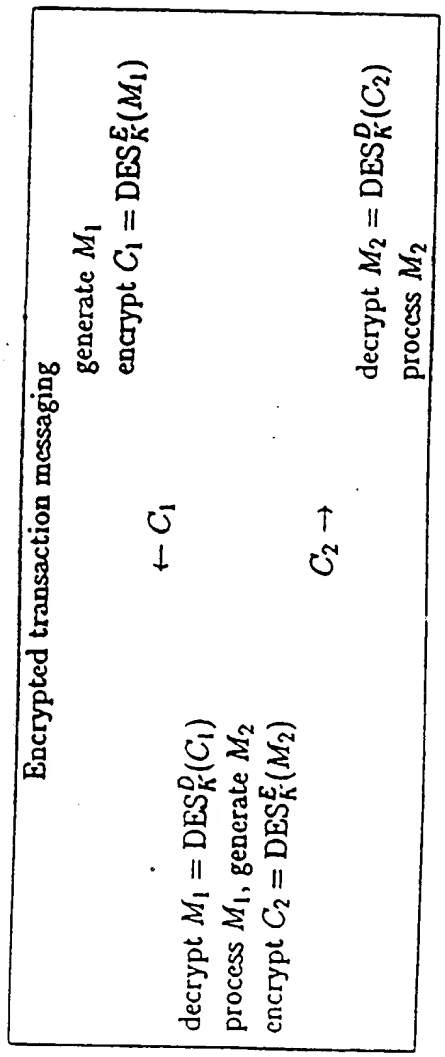


Figure 5(c)

P-ATM	KDS	Service Server
Initial configuration		
ID_u	ID_k, d_k, Q_k	d_s, Q_s
Online P-ATM to server binding		
generate x, tP, tQ_k	connect →	
	← query ID (y)	generate y
	(ID_u, x, tP) →	lookup ID_u
$K = \text{SHA}(x\|\|y\|\|tQ_s\|\|ID_u)$		compute $d(tP) \equiv tQ_k$
		$K = \text{SHA}(x\|\|y\|\|d(tP)\|\|ID_u)$
		generate $M_1 = Q_s$
verify	← $(M_1, S_K(M_1))$	$S_K(M_1) = \text{DES}_K^E(M_1)$
$S_K(M_1) \equiv \text{DES}_K^E(M_1)$		
program $Q_s = M_1$		
generate $M_2 = \text{ACK}$		
$S_K(M_2) = \text{DES}_K^E(M_2)$	$(M_2, S_K(M_2))$ →	verify $S_K(M_2) = \text{DES}_K^E(M_2)$
		update database
KDS to server distribution		
	generate x, tP, tQ_s	connect →
		← query ID (y)
		(ID_k, x, tP) →
	$K = \text{SHA}(x\|\|y\|\|tQ_k\|\|ID_k)$	
		generate M_1 = Update query
	verify $S_K(M_1) \equiv \text{DES}_K^E(M_1)$	← $(M_1, S_K(M_1))$
	generate $M_2 = (ID_u, Q_u)$	
	$S_K(M_2) = \text{DES}_K^E(M_2)$	$(M_2, S_K(M_2))$ →
P-ATM to server access		
generate x, tP, tQ_s	connect →	
		← query ID (y)
	(ID_u, x, tP) →	
$K = \text{SHA}(x\|\|y\|\|tQ_s\|\|ID_u)$		
verify $S_K(M_1) \equiv \text{DES}_K^E(M_1)$		← $(M_1, S_K(M_1))$
process M_1, generate M_2		
compute $S_K(M_2) = \text{DES}_K^E(M_2)$		
	$(M_2, S_K(M_2))$ →	

Service Server
generate y
lookup ID_k
compute $d(tP) \equiv tQ_k$
$K = \text{SHA}(x\|\|y\|\|d(tP)\|\|ID_k)$
generate M_1 = Update query
$S_K(M_1) = \text{DES}_K^E(M_1)$
verify
$S_K(M_2) = \text{DES}_K^E(M_2)$
add (ID_u, Q_u) to database
generate y
lookup ID_u
compute $d(tP) \equiv tQ_s$
$K = \text{SHA}(x\|\|y\|\|d(tP)\|\|ID_k)$
$S_K(M_1) = \text{DES}_K^E(M_1)$
verify $S_K(M_2) = \text{DES}_K^E(M_2)$

Figure 6:

P-ATM/SAM	Service Server	KDS
Initial configuration		
ID_u, d_u, Q_u $SAK = TDES^{E}_{K_V}(ID_u, Q_u)$	d_s, Q_s	$(ID_u, Q_u), Q_s, K_V$
Registration/Binding		
Register		Bind ID_u to Q_s $SAK = TDES^{E}_{K_V}(ID_u, Q_u)$ $ESK = DES^{E}_{SAK}(ID_u, Q_s)$
FIGURE 4(a)	Update database $S_R(M)$ with $(ID_u, Q_u), ESK$ $\leftarrow M$	$M = (ID_u, Q_u, ESK)$
First connection		
	connect →	
	← query ID (y)	generate y
$h = \mathrm{SHA}(x \Vert y \Vert tP \Vert ID_u)$ $s = S_c(h)$	(ID_u, x, tP, s) →	
		lookup Q_u using ID_u
	← ESK	
$(ID, Q_s) = DES^{D}_{SAK}(ESK)$ Verify $ID \equiv ID_u$ Program Q_s		FIGURE 4(b)

8058 P-ATM		Server
Initial configuration		
ID_u, Q_s		ID_u, d, Q_s
Call establishment		
generate x, tP, tQ_s	establish link $\rightarrow$	
		generate y
	$\leftarrow$ query identity (y)	
	$(ID_u, x, tP) \rightarrow$	
$K = \mathrm{SHA}(x\|\|y\|\|tQ_s\|\|ID_u)$		lookup ID_u
		compute $d(tP) \equiv tQ_s$
		$K = \mathrm{SHA}(x\|\|y\|\|d(tP)\|\|ID_u)$

FIGURE 5 (a)

Verifiable transaction messaging		
		generate M_1
		compute $S_K(M_1) = \mathrm{DES}_K^E(M_1)$
	$\leftarrow (M_1, S_K(M_1))$	
verify $S_K(M_1) \equiv \mathrm{DES}_K^E(M_1)$		
process M_1, generate M_2		
compute $S_K(M_2) = \mathrm{DES}_K^E(M_2)$		
	$(M_2, S_K(M_2)) \rightarrow$	
		verify $S_K(M_2) = \mathrm{DES}_K^E(M_2)$
		process M_2

FIGURE 5 (b)

P-ATM/SAM		KDS	Service Server
		Initial configuration	
ID_u, d_u, Q_u, Q_k		ID_k, d_k, Q_k	d_s, Q_s
		Online P-ATM to server binding	
generate x, tP, tQ_k	connect →		
	← query ID (y)	generate y	
$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$			
$s = S_c(h)$	(ID_u, x, tP, s) →	lookup Q_u using ID_u	
$K = \mathrm{SHA}(tQ_k\|\|x\|\|y)$		$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$	
		verify $h, S_c(h)$ with Q_u	
		compute $d(tP) \equiv tQ_k$	
		$K = \mathrm{SHA}(d(tP)\|\|x\|\|y)$	
		generate $M_1 = Q_s$	
verify	← $(M_1, S_K(M_1))$	$S_K(M_1) = \mathrm{DES}_K^E(M_1)$	
$S_K(M_1) \equiv \mathrm{DES}_K^E(M_1)$			
program $Q_s = M_1$			
generate $M_2 = \mathrm{ACK}$			
$S_K(M_2) = \mathrm{DES}_K^E(M_2)$	$(M_2, S_K(M_2))$ →	verify $S_K(M_2) = \mathrm{DES}_K^E(M_2)$	
		update database	

FIGURE 3(a)

KDS to server distribution			
generate x, tP, tQ_s	connect →		
		← query ID (y)	generate y
$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_k)$ $s = S_e(h)$ $K = \mathrm{SHA}(tQ_k\|\|x\|\|y)$		(ID_k, x, tP, s) →	lookup Q_k using ID_k $h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_k)$ verify $h, S_e(h)$ with Q_k compute $d(tP) \equiv tQ_k$ $K = \mathrm{SHA}(d(tP)\|\|x\|\|y)$
			generate M_1 = Update query
verify $S_K(M_1) \equiv \mathrm{DES}_K^E(M_1)$ generate $M_2 = (ID_u, Q_u)$ $S_K(M_2) = \mathrm{DES}_K^E(M_2)$		← $(M_1, S_K(M_1))$ $(M_2, S_K(M_2))$ →	$S_K(M_1) = \mathrm{DES}_K^E(M_1)$ verify $S_K(M_2) = \mathrm{DES}_K^E(M_2)$ add (ID_u, Q_u) to database

FIGURE 3C b)

P-ATM to server access			
generate x, tP, tQ_s	connect →		
		← query ID (y)	generate y
$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$ $s = S_e(h)$ $K = \mathrm{SHA}(tQ_s\|\|x\|\|y)$	(ID_u, x, tP, s) →		lookup Q_u using ID_u $h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$ verify $h, S_e(h)$ with Q_u compute $d(tP) \equiv tQ_s$ $K = \mathrm{SHA}(d(tP)\|\|x\|\|y)$
verify $S_K(M_1) \equiv \mathrm{DES}_K^E(M_1)$ process M_1, generate M_2 compute $S_K(M_2) = \mathrm{DES}_K^E(M_2)$		← $(M_1, S_K(M_1))$	$S_K(M_1) = \mathrm{DES}_K^E(M_1)$
	$(M_2, S_K(M_2))$ →	Figure 3(c)	verify $S_K(M_2) = \mathrm{DES}_K^E(M_2)$

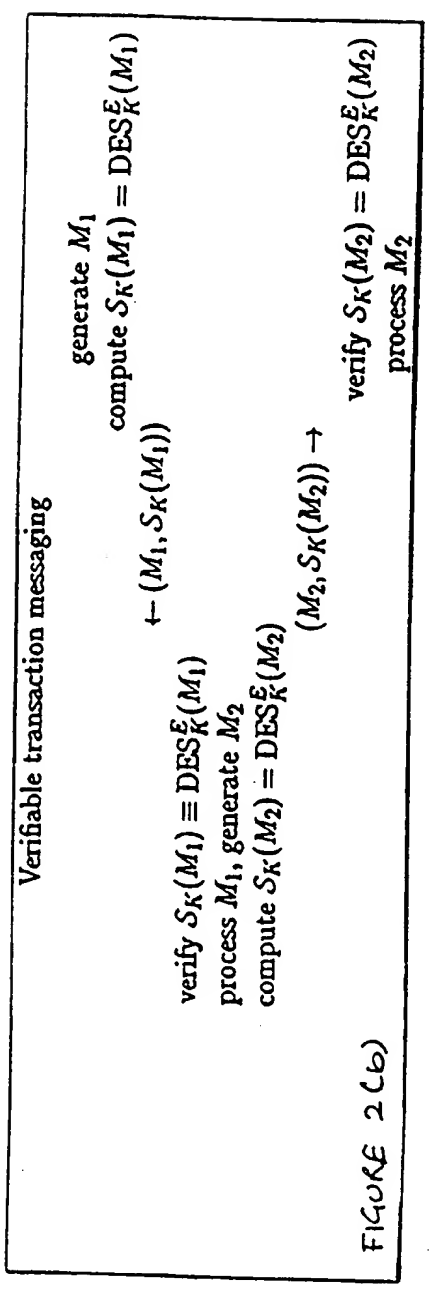


FIGURE 2(b)

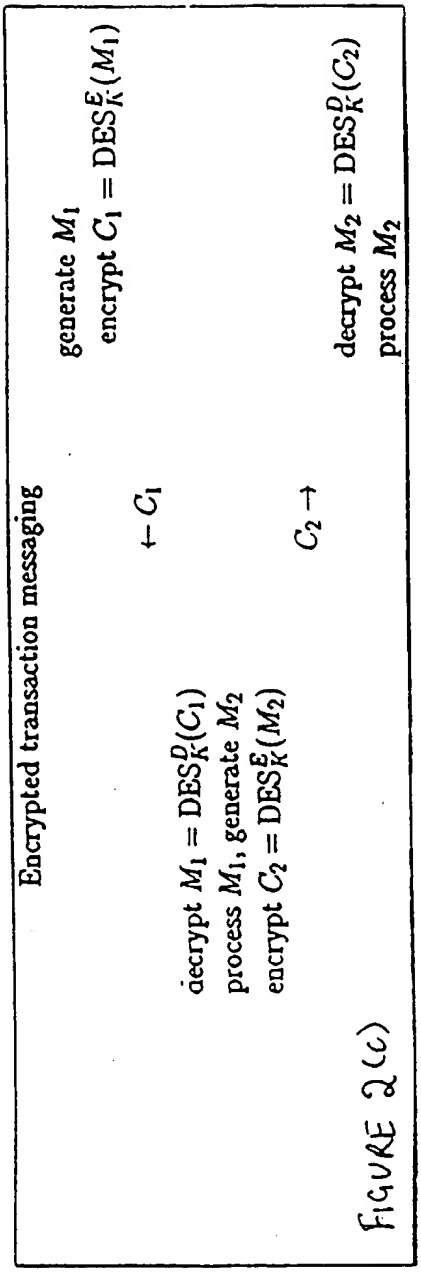


FIGURE 2(c)

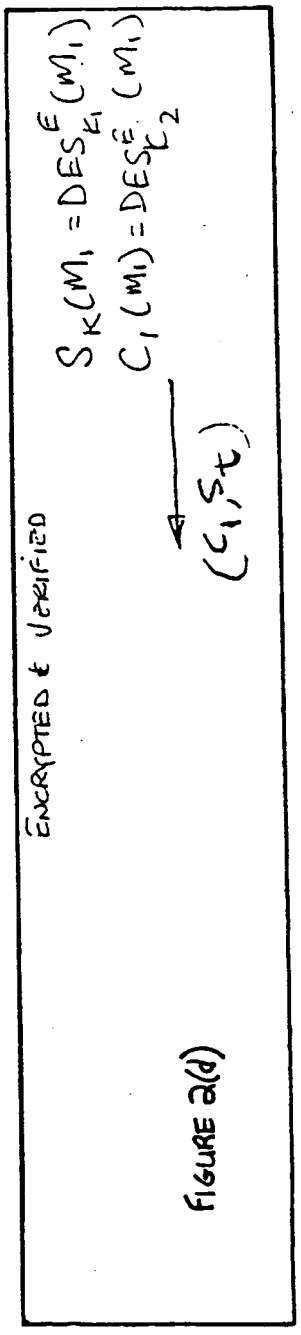


FIGURE 3(d)

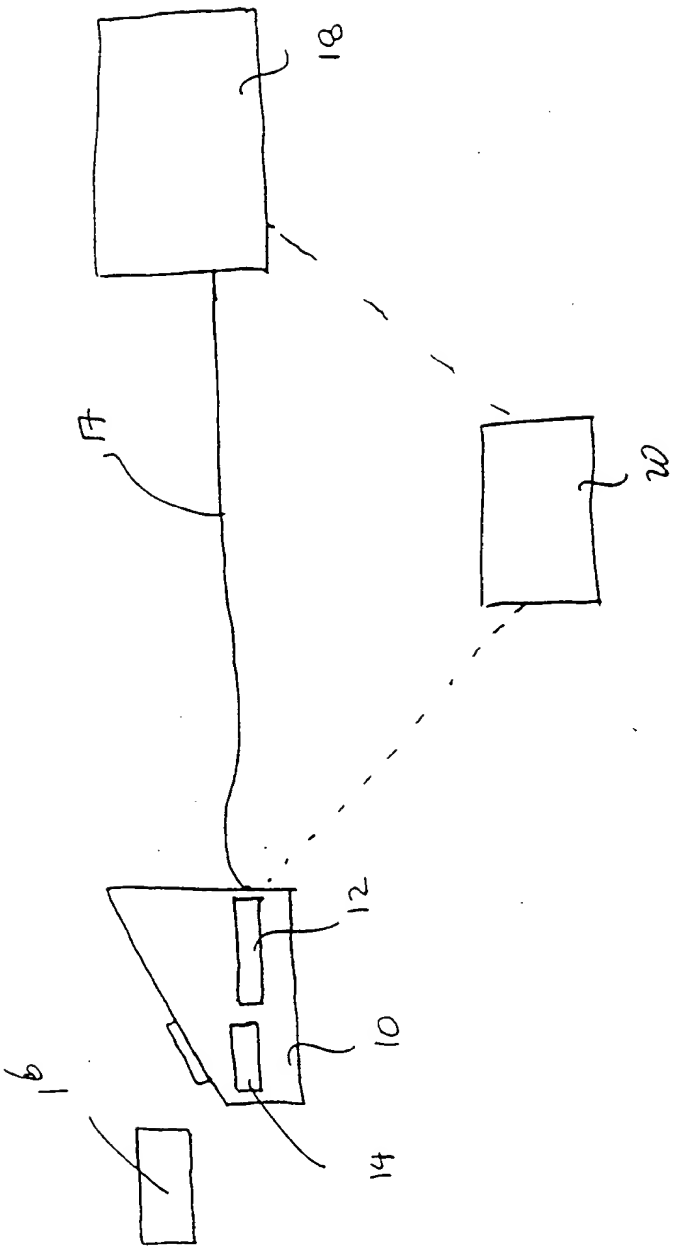


FIGURE 1.

SAM	8058 P-ATM		Server
		Initial configuration	
c, Q_u	ID_u, Q_s		$(ID_u.Q_u), d, Q_s$
		Call establishment	
	generate x, tP, tQ_s	establish link →	
			generate y
		← query identity (y)	
	$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$		
	← h		
compute $S_c(h)$			
	$S_c(h)$ →		
		$(ID_u, x, tP, S_c(h))$ →	
	$K = \mathrm{SHA}(tQ_s\|\|x\|\|y)$		look-up Q_u using ID_u
			$h = \mathrm{SHA}(x\|\|y\|\|tP\|\|ID_u)$
			verify $h, S_c(h)$ with Q_u
			compute $d(tP) = tQ_s$
			$K = \mathrm{SHA}(d(tP)\|\|x\|\|y)$

FIGURE 2(a)

and said generator being a point P on said elliptic curve.

14. A method as defined in claim 1, said second correspondent being a key distribution server.

15. A method as defined in claim 1, said first correspondent being a terminal and second correspondent being a server.

16. A method of authenticating a pair of correspondents C,S to permit the exchange of information therebetween, each of said correspondents having a respective private key, e, d and a public key, Q_u and Q_s derived from a generator element of a group and a respective ones of said private keys e,d, said method comprising the steps of:

i. a first of said correspondents C generating a session value x;

ii. said first correspondent generating a private value t, a public value derived form said private value t and said generator and a shared secret value derived from said private value t and said public key Q_s of said second correspondent;

iii. said second correspondent generating a challenge value y and transmitting said value y to said first correspondent;

iv. said first correspondent in response thereto transmitting said challenge value y, said session value x, said public value an of said first correspondent; and

v. said second corresponding verifying a corresponding stored identity to thereby verify said first correspondent.

17. A method of authenticating a pair of correspondents C,S to permit exchange of information therebetween, each of said correspondents C,S having a respective private key e,d and a public key Q_u and Q_s derived from a generator P and a respective ones of said private keys e,d, a list of said correspondents C having a unique identification information ID_u stored therein, said a second of said correspondent a including a

memory for storing public keys of one or more of said first correspondents, said method comprising steps of:

a) said second of said correspondents generating a random value y upon initiation of a transaction between said correspondents;

b) said second correspondent S forwarding to said first correspondent C said value y;

c) said first correspondent C generating a first random number x and computing a public session key tP from a private key t;

d) said first correspondent C generating a message H by combining said first random number x, said value y, said public session key tP and said unique identification information ID_u and computing a signature S_e of said message H;

e) said first correspondent C transmitting said signature S_e, said public session key tP, said value x and said identification ID_u to said second correspondent;

f) said second correspondent upon receipt of said message from said previous step (Q) retrieving said public key Q_u of said first correspondent from said memory using said received identification information ID_u; and

g) said second correspondent verifying said received signature using said recovered public key Q_u and verifying said message H and computing a shared secret key d(tP), whereby both said correspondents may calculate a shared secret key k by combining the computed secret $tQ_s = d(tP)$ with said first random number x and said random value y, said key K being utilized in subsequent transactions between said correspondents for a duration of said session.

THE EMBODIMENTS OF THE INVENTION IN WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED ARE DEFINED AS FOLLOWS:

1. A method of authenticating a pair of correspondents C.S to permit the exchange of information therebetween, each of said correspondents having a respective private key, *e. d* and a public key, Q_u and Q_s derived from a generator element of a group and a respective ones of said private keys *e.d*, said method comprising the steps of:

i. a first of said correspondents *C* generating a session value *x*;

ii. said first correspondent generating a private value *t*, a public value derived from said private value *t* and said generator and a shared secret value derived from said private value *t* and said public key Q_s of said second correspondent;

iii. said second correspondent generating a challenge value *y* and transmitting said challenge value *y* to said first correspondent;

iv. said first correspondent in response thereto computing a value *h* by applying a function *H* to said challenge value *y*, said session value *x*, said public value an of said first correspondent;

v. said first correspondent signing said value *h* utilizing said private key *e*;

vi. said first correspondent transmitting to said second correspondent said signature including said session value *x*, and said private value *t*; and

vii. said second correspondent verifying said signature utilizing said public key Q_u of said first correspondent and whereby verification of said signature authenticates said first correspondent to said second correspondent.

2. A method as defined in claim 1, including said second correspondent computing said shared secret value by utilizing its private key *d* and said public value and said first and second correspondents computing a session key *k* derived from said shared secret, said session value *x* and said challenge value *y*.

3. A method as defined in claim 1, said signature forwarded by said first correspondent includes an identification ID_u of said first correspondent.

4. A method as defined in claim 1, said first correspondent including a general purpose computer and a signature module for computing said signature.

5. A method as defined in claim 4, said private and public keys of said first correspondent being embedded within said signature module and said private key being accessible by a signature function.

6. A method as defined in claim 5, said identification ID_u being stored within said general purpose processor.

7. A method as defined in claim 1, said public value being a Diffie-Hellman public value.

8. A method as defined in claim 1, said group being an elliptic curve group $E(F_q)$ and said generator element being a point P on said elliptic curve.

9. A method as defined in claim 1, said second correspondent utilizing said identification ID_u for retrieving said public key Q_u from a database.

10. A method as defined in claim 9, said session key k including a usage code value for specifying a transaction type in a given session.

11. A method as defined in claim 1, said function H being a hash function.

12. A method as defined in claim 1, including transmitting a verifiable message between said correspondents by appending thereto a data encryption standard authentication code using said computed session key.

13. A method as defined in claim 1, said group being an elliptic curve group $E(F_2^m)$

unique number (x) and the Diffie-Hellman public value (tP). In contrast to the embodiment shown in figure 2, where the response includes the signature component.

As previously shown, ID_u will be checked in the database. If it exists, the server now knows that it is communicating with a legitimate P-ATM. The transaction number x may be verified unique if possible (for example, if x is a transaction number, make sure it is larger than the last transaction number). The Diffie-Hellman shared secret tQ_s will be computed from the transmitted value tP using the server's private key d. From the shared secret and both the server and P-ATM session-unique values a session key is derived:

$$K = \mathrm{SHA}(x \| y \| d(tP) \| ID_u \| \text{"}MAC\text{"}) \text{ or } \| \text{"}ENC\text{"} \text{ or both or null.}$$

This completes the secure call establishment as is more clearly seen with reference to figure 5(a).

Once a secure call has been established between the P-ATM and the server, transaction messages in either direction can now be made verifiable by appending a DES MAC using the computed session key shown in figure 5(b) and 5(c). Alternatively, messages can be made private by encrypting them with that key instead of MACing them. If only authentication is required, the message recipient must recompute the MAC from the message and accept it only if the MACs agree. If encryption is desired, the plaintext message must be decrypted from the ciphertext message received or both.

In the case of P-ATMs not manufactured with SAM modules it is still necessary to perform P-ATM to server binding to issue the appropriate server public key to the P-ATM and to issue the P-ATM ID to the appropriate server. Both of these actions must be done securely. As with the SAM module P-ATM previously described, two methods of key distribution may be implemented. The two phase public key distribution method, as shown in figure 6, once again assumes that a key distribution server (KDS) exists which issues binding information to the appropriate server for each P-ATM. The P-ATMs are preloaded with a server authentication key (SAK) generated by the KDS at manufacture time. The KDS uses the same triple-DES key to generate unique SAKs for all P-ATMs.

Alternatively, a single phase symmetric key distribution method is illustrated in figure 7. The P-ATMs are preloaded with a unique (DES) server authentication key

(SAK) at manufacture time. This key will authenticate the server public key the first time a connection is established. A connection must be established from the KDS to a server for each P-ATM being bound to that server. The KDS maintains a solitary triple-DES key with which the P-ATM server authenticating keys (SAKs) are generated. This key distribution then proceeds similarly to that described with reference to the embodiment shown in figure 4.

While the above protocols have been described with reference to specific embodiments thereof and in a specific use, various modifications thereof will occur to those skilled in the art without departing from the spirit of the invention. For example, other symmetric key schemes, instead of DES and triple DES, may be implemented, similarly equivalent hash functions, possibly derived from DES may be implemented instead of SHA1. The protocols provide secure generation and loading of keying material at both the time of manufacture of the P-ATM and the initial communication with its assigned server. They also provide mutual authentication of the P-ATM and server on a per session basis.

signature functions. The public key Q_u can be read by the P-ATM. The P-ATMs are preloaded with a public key Q_u of the KDS at manufacture time. A connection must be established once from each P-ATM to the KDS in order to bind that P-ATM to the appropriate server. A connection must be established from the KDS to the server for each P-ATM being bound to that server.

Consider the initial state of the three distinct entities: KDS 20, P-ATM 10, and server 18. The KDS is installed and constructs its key pair (d_k, Q_k) prior to the manufacture of P-ATMs. Each P-ATM is manufactured with a SAM containing the key pair (d_u, Q_u), and with the KDS public key Q_k embedded within its ROM. At some time in the future, the server 18 is installed and constructs its private, public key pair (d_s, Q_s). When this occurs, the KDS is informed of the server's public key (Q_s) and any localization information about the server (service type, geographic coverage, etc.).

Once a P-ATM is delivered to the customer it must be bound to a server before it can be used for its intended purpose. This is accomplished by first establishing a connection from the P-ATM 10 to the KDS 20. This can be done using the same communications mechanisms, protocols, and cryptography as a P-ATM-to-server connection. Once this connection is established, the P-ATM can issue its public key Q_u to the KDS 20 and the KDS 20 can issue the appropriate server's public key Q_u to the P-ATM 10. The appropriate server is determined by the application in which the P-ATM 10 is to be used. For example, it could be a function of where the P-ATM was purchased. Specification of the intended function for the P-ATM could be either inband or out of band.

Subsequent to this connection, the P-ATM now knows the server to which it will make a connection. The server must be informed of the new P-ATM that it must recognize. This can be done by the KDS making a secure connection with the server (again, using the same P-ATM-to-server protocol) as if it were a P-ATM. The new binding information may conveniently be stored in a database within the server and is then integrated into the server's world-view. This database update connection can occur either as a batch operation at the end of each week, in real-time on a per binding basis, or at some time in between these extremes.

In another embodiment, a single phase symmetric key distribution method is described with reference to figure 4. In this embodiment as with the previous

embodiment, the SAM modules are pre-keyed by the SAM manufacturer. The private key d_u can only be accessed by the signature function. The public key Q_u can be read by the P-ATM. The P-ATMs are preloaded with a unique (DES) server authentication key (SAK) at manufacture time. This key will authenticate the server public key Q_s the first time a connection is established to the P-ATM. A connection must be established to a server for each P-ATM being bound to that server. The KDS 20 maintains a solitary triple-DES key K_v with which the P-ATM server authenticating keys (SAKs) are generated.

Consider the initial state of the P-ATM 10 and server 18. Each P-ATM is manufactured with a SAM containing the key pair (d_u, Q_u), and with a unique identifier ID_u. During manufacture, each P-ATM's identity defined by its unique identifier ID_u and public key Q_u (ID_u, Q_u) is encrypted under the triple-DES key K_v to produce a $SAK = TDES_{K_v}^{E}(ID_u, Q_s)$. Each P-ATM obtains a unique SAK because the P-ATM identities are all distinct. At some time in the future, a client server is installed and constructs its key pair (d_s, Q_s). When this occurs, the KDS 20 is informed of the server's public key (Q_s) and any localization information about the server (service type, geographic coverage, etc.).

Once a P-ATM is delivered to the customer it must be bound to the server before it can be used for its intended purpose. Registering the P-ATM device with the KDS binds the P-ATM to the appropriate server. In order to notify the server of the newly legitimized P-ATM, that server is sent the P-ATM's identity ID_u and public key Q_u. In order for the P-ATM to accept the server as legitimate the first time a connection is established, the P-ATM's identity and server's public key Q_s are encrypted with the P-ATM's SAK ($ESK = DES_{SAK}^{E}(ID_u, Q_s)$) and sent to the server as an update to its database. This transport can be easily used to protect server updates.

The server will issue the encrypted key to the P-ATM where it is verified using the SAK as shown in figure 4(b). The SAK need not be securely stored at manufacture time for this purpose; it is possible to reconstruct the SAK using the ID and public key of the P-ATM and the triple-DES key which only the KDS has.

In another embodiment, the P-ATM may not have a SAM module embedded within it. In this case, as shown in figure 5(a), the P-ATM's response to the server's "who-are-you?" challenge will include its identification string (ID_u) and its transaction-

server, once it receives a call request from the P-ATM, will generate a random session value y and queries the identity of the P-ATM.

Generally, when the P-ATM establishes a call to the server, the server will generate a "who-are-you?" challenge to the P-ATM. The P-ATM's response to the server's "who-are-you?" challenge will include the following information: its serial number and/or equivalent identification string (ID_u) (this will be used for public key lookup at the server); the session unique number (x) (this must be a statistically unique number but not necessarily non-deterministic); the Diffie-Hellman public value (tP); and a signature $S_e(h)$ of the hash $h = SHA(y \| x \| tP \| ID_u)$ signed by the private key e of the SAM. The P-ATM will thus send (ID_u, x, tP, $S_e(h)$) to the server. The SHA is generally an SHA-1 hash function.

At whatever point tP is computed (just prior to the call, several sessions previous, or as a one time computation), it is also necessary to compute tQ_s.

At the server, ID_u will be used to look up Q_u from a database of stored public keys of literally thousands of P-ATMs. The value x may be verified to be unique if possible (for example, if x is a transaction number, make sure it is larger than the last transaction number). The values x, tP, and ID_u will be used to reconstruct the hashed message $h = SHA(y \| x \| tP \| ID_u)$. The hash h will then be used to verify the signature using the public key Q_u recovered from the database. Assuming all is successful, the server now knows that it is communicating with a legitimate P-ATM.

The server must now construct the Diffie-Hellman shared secret tQ_s. This is done with its private key d to compute:

$$tQ_s \equiv d(tP).$$

From the shared secret $d(tP)$ and both the server and P-ATM session-unique values y and x, respectively, a session key k is derived from a hash of $(d(tP) \| x \| y \|$ usage code), were the usage code may be a string specifying "MAC" or "ENC," or if only one, then it is set to null. The user of the P-ATM would decide whether to use "MAC" or "ENC," e.g. for transactions over $1000 - use "ENC" or use "MAC," otherwise:

$$K = SHA(d(tP) \| x \| y \| "MAC") \text{ or } \| "ENC".$$

Set up by a user profile for example stored in the cash card when it is issued by the institution.

Transaction messages in either direction can now be made verifiable by appending a data encryption standard message authentication code (DES MAC) using the computed session key K_{MAC} as shown in figure 2(b). Alternatively as shown in figure 2(c), messages can be made private by encrypting them with the key K_{ENC} instead of MACing. If only authentication s required, the message recipient must recompute the MAC from the message and accept it only if the MACs agree. If encryption is desired, the plaintext message must be decrypted from the ciphertext message received. If both encryption and verification is required, then both encryption and MACing may be employed as shown in figure 2(d). With the above protocol, it may be seen that service storage, computation and speed constraints of the P-ATM are overcome since it performs relatively simple operations. For example, the computation of a hash is relatively easy, whereas the dedicated SAM performs the signature function. Similarly, the verification of the DES MAC is relatively easy for the P-ATM to perform. Thus, security is achieved by the P-ATM and server computing and using a shared secret that ensures the accuracy of each session.

Turning now to figure 3, as outlined earlier, in order to simplify the manufacturing process for P-ATMs, the mapping of P-ATMs to their servers is unknown until the customer purchases a device. It is anticipated that servers may service in the order of 100,000 P-ATMs. To perform P-ATM to server binding it is necessary to issue the appropriate server public key Q_s to the P-ATM and to issue the P-ATM public key Q_u and identity information ID_u to the appropriate server. Both of these actions must be performed securely. This may be achieved by either a two phase method using public key cryptography which uses the previously defined secure protocol for P-ATM to server messaging or a one phase method using symmetric key cryptography.

A two phase public key distribution method is described with reference to figure 3. In this embodiment, a key distribution server (KDS) 20 exists, as shown in figure 1, which is used to bind P-ATMs 10 to their long-term servers 18. The SAM modules 12 within the P-ATMs 10 are pre-keyed with their private key e and public key Q_u by the SAM manufacturer. The private key e can only be accessed from within the SAM by a

first random number x and said random value y, said key K being utilized in subsequent transactions between said correspondents for a duration of said session.

Also, this aspect of the invention provides for apparatus for carrying out the method. Such an apparatus can comprise any computational apparatus such as a suitably programmed computer.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other features of the present invention will become more apparent from the following description of preferred embodiments of the invention, which are described by way of example, only, with reference to the accompanying drawings in which like elements have been assigned like numbers and wherein:

Figure 1 is a schematic diagram of P-ATM server configuration;

Figures 2 (a), (b), (c) and (d) are schematic diagrams of an authentication protocol between a server and a personal ATM;

Figures 3 (a), (b) and (c) are schematic diagrams of a two phase public key distribution system;

Figures 4 (a) and (b) are schematic diagrams of a single phase symmetric key distribution system;

Figures 5 (a), (b) and (c) are schematic diagrams showing a protocol for establishing a secure session without a sign only module;

Figure 6 is a further embodiment of a two phase public key distribution system; and

Figure 7 is a further embodiment of a single phase symmetric key distribution system.

DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

Referring to figure 1, a personal ATM (P-ATM) 10 has sign only module (SAM) chip 12, such as a SC27 or SC46, embedded therein. The P-ATM also includes an 8058 8-bit processor chip 14 which is only capable of performing simple calculations due to its low processing power. The SAM module generally has elliptic curve (EC) sign-only capabilities and is generally available in "smart-cards" and the

like. The P-ATM 10 is connected via a suitable communication channel 17 to a service server 18. A cash card 16 may be used to access services provided by the server 18 via the P-ATM 10.

Message exchange between the P-ATM 10 and the server takes place using public key encryption. For the sake of clarity, the following terms which are used in the following description, are defined:

P – A generator point on an elliptic curve.

ID_u – A string that uniquely identifies the P-ATM 10, this string is stored within the 8058 firmware.

e, Q_u – A private (signature) and public keys of the SAM embedded within a P-ATM device. The public key Q_u is obtained from the private key e.

d, Q_s – Private and public keys of the server 18.

x – A session random value generated by a P-ATM device.

y – A session random value generated by the server 18.

M – A plaintext message of arbitrary content in either direction between the P-ATM and server.

SHA(M) – The hash of a message M using SHA-1.

$DES_K^E(M)$ – The ciphertext generated by encrypting plaintext M with DES using a key K.

$DES_K^D(E)$ – The plaintext generated by decrypting ciphertext E with DES using a key K.

$S_e(M)$ – A signature generated by signing message M with private key e.

t – A Diffie-Hellman private value generated by the P-ATM used to generate a shared secret tQ_s. The value of t may be precomputed and/or reused over multiple sessions.

Referring now to figure 2 (a), it is assumed that the SAM, the P-ATM and the server have already been initialized with the appropriate parameters. This will be discussed later. A session is established by the P-ATM initiating a call to the server on the request of a user. For each session, the P-ATM generates a random session unique value x and computes tP (the Diffie-Hellman shared secret) and tQ_s. The value t is the Diffie-Hellman private value used to generate the eventual shared secret tQ_s. The

TWO WAY AUTHENTICATION PROTOCOL

This invention relates to a protocol for verifying parties in a transaction and, in particular, cryptographic protocols for providing secure personal ATM transactions between an electronic device and a server and in which the protocols are based on a public key algorithm.

BACKGROUND OF THE INVENTION

With advent of electronic commerce, the use of cash in financial transactions in becoming less popular, in favour of electronic wallets. Typically, a financial institution will issue its customers with a personal ATM device (P-ATM) and an electronic cash card. The user then uses the electronic cash card, which stores a cash amount thereon, in various financial transactions. The cash card communicates with the financial institution's central server via the personal ATM. Because there is less control exercised by a financial institution on a P-ATM than a regular ATM installed, for example, at a bank site, it is necessary for the P-ATMs to be authenticated both by the issuing financial institution as well as by the cash card user in addition to the usual verification of the cash card used by the institution and sometimes vice versa.

In order to simplify the manufacturing process for personal ATMs, the mapping of a P-ATM's cryptographic parameters to a server is unknown until the customer purchases the P-ATM device. To perform P-ATM to server binding, it is necessary to issue the appropriate server public key to the P-ATM and to issue the P-ATM public key and ID to the appropriate server. Both of these actions must be done securely. The difficulty in the authentication presented by this type of application is that the cash card must trust the server and vice versa. Thus, it is necessary that the server then verify the P-ATM and vice versa. Once the server and the P-ATM trust each other, the user can then use the cash card with the ATM with relative confidence. Furthermore, these verifications must be performed relatively quickly. Thus, there is a need for a verification and authentication protocol that meets the needs of this type of transaction.

SUMMARY OF THE INVENTION

This invention seeks to provide a verification and authentication protocol that enables at least one party in at least a three party transaction to be authenticated by the remaining parties.

Furthermore this invention seeks to provide an authentication protocol in a cash-card, personal ATM and server transaction.

This invention also seeks to provide a key distribution method for personal ATM's and the like.

In accordance with an aspect of the invention there is provided a method of authenticating a pair of correspondents C,S to permit exchange of information therebetween, each of said correspondents C,S having a respective private key e,d and a public key Q_u and Q_s derived from a generator P and a respective ones of said private keys e,d, a list of said correspondents C having a unique identification information ID_u stored therein, said a second of said correspondent a including a memory for storing public keys of one or more of said first correspondents, said method comprising steps of:

a) said second of said correspondents generating a random value y upon initiation of a transaction between said correspondents;

b) said second correspondent S forwarding to said first correspondent C said value y;

c) said first correspondent C generating a first random number x and computing a public session key tP from a private key t;

d) said first correspondent C generating a message H by combining said first random number x, said value y, said public session key tP and said unique identification information ID_u and computing a signature S_e of said message H;

e) said first correspondent C transmitting said signature S_e, said public session key tP, said value x and said identification ID_u to said second correspondent;

f) said second correspondent upon receipt of said message from said previous step (Q) retrieving said public key Q_u of said first correspondent from said memory using said received identification information ID_u;

g) said second correspondent verifying said received signature using said recovered public key Q_u and verifying said message H and computing a shared secret key d(tP), whereby both said correspondents may calculate a shared secret key k by combining the computed secret $tQ_s = d(tP)$ with said